Network Information Security Risk Assessment Method Based on Machine Learning Algorithm

Ruirong Jiang(✉) and Liyong Wan

Jiangxi University of Software Professional Technology, Nanchang 330041, China
jiangruirong632@163.com

Abstract. The current computer network information security risk assessment methods have the problems of low assessment accuracy, which seriously restricts the assessment effect. In order to solve this problem and improve the effect of network information security risk assessment and the level of network information security, this paper designs a network information security risk assessment method based on network learning algorithm. Describe the risk calculation form, extract the performance characteristics of network information, identify the network risk factors, draw conclusions according to logical reasoning, adopt computer network risk control and defense measures, use machine learning algorithm to build a security system model, and optimize the security risk assessment mode. The experimental results prove that the highest accuracy rate of the network information security risk assessment method is 95.612%, indicating that the network information security risk assessment method is more practical after combining the machine learning algorithm.

Keywords: Machine learning · Network information · Security risk · Risk assessment · Security defense · Security risks

1 Introduction

With the rapid development and popularization of computer technology, computer network has increasingly become a bridge for people to learn and communicate, and gradually become an indispensable tool in people's daily life. Information resources can be shared through the network, which not only expands the space and time, but also improves the efficiency of work or learning. But with the rapid expansion of the network, the number of cyber security accidents and the losses are also spreading. However, in the field of computer and network security, it is difficult to symmetry the security risk assessment research and results of network system with its importance. Network information security has gradually become the focus of people's attention, and the core of network security is the risk assessment of the network system [1–3]. Network risk assessment, also known as security risk assessment and network security risk assessment, refers to the whole process of detecting, identifying, controlling and eliminating the known or potential security risks and security risks in the network, and is one of the necessary measures for enterprise network security management.

W. Fu and L. Yun (Eds.): ADHIP 2022, LNICST 469, pp. 403–416, 2023.
https://doi.org/10.1007/978-3-031-28867-8_30

Risk assessment is from the perspective of risk management, using scientific methods and means to systematically analyze the threats to the network and information system and their vulnerabilities, and evaluate the degree of harm caused by security events. Through the network security assessment, we can comprehensively sort out the assets in the network, understand the existing security risks and hidden dangers, and carry out targeted security reinforcement to ensure the safe operation of the network. Network security refers to the information security on the network, which means that the hardware and software of the network system and its data in the system are protected, the system operates continuously, reliably and normally, there is no damage, change or leakage due to accident or malicious reasons, and the network service is not interrupted. Therefore, in the face of the rapid growth of computer network information security needs, only passive defense technology can not meet the network security defense, and can not fundamentally solve the network security defense problem. It is necessary to comprehensively prevent and control the security of information systems.

Network security is essentially the information security on the network. In a broad sense, all the related technologies and theories involving the confidentiality, integrity, availability, authenticity and controllability of the information on the network are the research fields of network security. Therefore, the computer network information security risk assessment can effectively analyze the current and future risk development trend and location of the network information system, evaluate the risks to the computer network information security threat and its impact degree, in order to better develop security defense strategy, provide safe operation guarantee for the computer network information. Network security involves content, technical and management issues, which are interrelated and indispensable. The technical focus is on how to prevent external illegal attacks, while the management side focuses on the management of internal human factors. How to protect the important information data more effectively and improve the security of the network system has become an important problem that must be considered and solved in the computer network applications. Put forward targeted protection countermeasures and rectification measures to control the risk at an acceptable level, so as to maximize the security of the network information system. Network security risk assessment is the basis and premise of ensuring network security, and it is of important research significance. However, the current computer network information security risk assessment methods have the problem of low accuracy, which seriously restricts the assessment effect. In order to solve this problem and improve the effect of network information security risk assessment and the level of network information security, this paper designs a network information security risk assessment method based on network learning algorithm.

2 Network Information Security Risk Assessment Method Based on Machine Learning Algorithm

2.1 Extract the Network Information Performance Features

Network security in essence, network security is the information security on the network, refers to the network system hardware, software and its data in the network system is protected, not because of accidental or malicious factors were destroyed, change, leakage, so as to make the system operate continuously, reliably and normally, the network service is not interrupted. To achieve this purpose, it is of vital significance to effectively evaluate the risks of information security. Only by effectively evaluating the security risks faced by the information system, can we fully grasp the security state of the information system, and take targeted risk control measures, so that the information security risks are within a controllable range.

Network security risk assessment refers to the process of scientific evaluation of the processing, transmission and storage of network information, as well as the confidentiality, integrity and availability of information, according to the relevant national network information security technical standards. In a security defense system, a perfect and reasonable security architecture is the core and foundation. The security architecture is usually based on the corresponding security conceptual model. As the primary link of the risk assessment project, the security model can be regarded as the first stage of the whole security framework, which is of great significance to the establishment of the whole security framework. To evaluate the vulnerability of the network information system, the threat faced, and the actual negative impact generated after the vulnerability is utilized by the threat source, and to identify the security risk of the network information system according to the possibility of security events and the degree of negative impact. Based on the assessment results, propose effective safety measures to eliminate or minimize the risk [4, 5]. Threat is the potential cause of accidents that may cause damage to assets or organizations, and risk assessment is concerned about the possibility of threat. Fulnerability is also known as vulnerability, which is the shortcomings of assets or asset groups that can be threatened. Frailty itself does not constitute harm, but once vulnerability is threatened, it may cause damage to the assets. It is not appropriate to temporarily put forward some information security risks in the information security risk assessment. We must determine the four elements of assets, threat, vulnerability and risk and their mutual relationship before the risk assessment under the premise of information risk management. The formal risk calculation principle is described as:

$$T = \frac{\delta(E, G, H)}{\sum_{i=1} |\delta_i - 1|^2} \tag{1}$$

In formula (1), δ represents the impact of an asset security event on the business of the institution, E represents the asset, G represents vulnerability, H represents threat, and i represents the vulnerability of an asset itself. Risk is the potential possibility of damage to the vulnerability of a specific threat. Risk is the result of the combination of the likelihood and impact of threat events. Assets are anything of value to an organization, including computer hardware, communications facilities, databases, document information, software, information services, and personnel, etc. It spreads throughout

the project work as the task is executed, and is consumed with the effective control measures taken by each sub-task. Through this model, some risks that are easily overlooked by traditional methods can be found. Therefore, determining the information security risk assessment model is the basis of risk assessment and the basis for effective risk assessment. It can provide methods and benchmarks for determining the risk size of the system. Asset value refers to the importance and sensitivity of assets. Asset value is the attribute of assets and also the specific content of asset appraisal. Security requirements refer to the requirements put forward in the information security measures to ensure the normal implementation of the business strategy of the unit. Security measures refer to various events, regulations and mechanisms implemented to deal with threats, reduce vulnerabilities, protect assets, limit the impact of accidents, discover and respond to accidents, promote disaster recovery and combat information crimes.

2.2 Identify Network Risk Factors

After statistical analysis, the current computer network security may encounter threats mainly from the following aspects: virus, Trojan, attack, vulnerability, encryption, eavesdropping. The complexity of information system determines the diversity, dynamics and uncertainty of security risk factors. However, this does not mean that the factors causing the safety events are completely unknown, and the rules can be found through the observation, statistics and analysis of a large number of risk event data. Usually, eavesdropping on the network, do not need to interrupt the network to transmit information, is called negative criminals. Malicious attackers often use this as a basis to recycle the remaining tools for more destructive attacks. Because network security risks involve a wide range of areas, complex nature and risk characteristics throughout the whole life cycle of the information system determine the great difficulty and complexity of their identification, and many interrelated and penetrating factors cannot be identified by observation and touch [6, 7]. Tampering is a legitimate user on the offense modifying, dele, deleting, inserts, and then sends forged information to the recipient, which is purely damaging between information communication, such cyber criminals are known as active criminals. The information package on the positive criminal Web is intercepted and modified, so that the information that favors oneself or is added deliberately is displayed. Risk analysis and assessors in unclear, incomplete, inaccurate, cannot completely according to logical reasoning and concluded to take some qualitative, fuzzy, effective risk factor identification method to as far as possible to collect, sorting, speculation data, and analysis of the actual situation, simulation, simulation and judgment, so as to find the potential, existing in the incomplete information. The basic structure of the safety risk assessment elements is shown in Fig. 1:

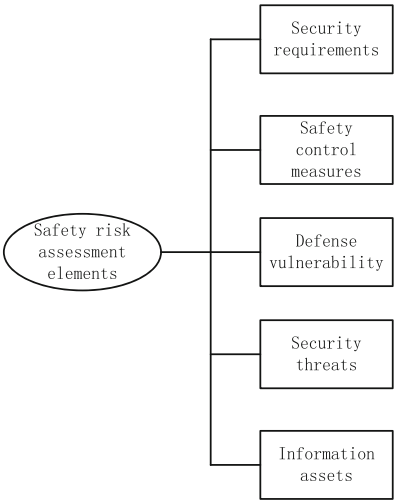

Fig. 1. Safety risk assessment elements

As shown in Fig. 1, security risk assessment elements include security requirements, security control measures, security threats, defense vulnerabilities, and information assets. A denial of service attack is an attack system that is slow or even paralyzed by some other means that can prevent access by legitimate users to the service. The conduct denial is that the communications entity denies that the act has occurred. Electronic deception is the purpose of killing the user's identity through counterfeiting legitimate cyber attacks, thus concealing the identity of the real attacker and blaming others. Then the obtained information is analyzed and sorted out, so as to determine the risk cause and the contribution of each factor to the system risk. According to the different starting points of risk factor identification, the identification methods are generally divided into two categories: one is to derive information and information system risks based on the security events that have occurred, and the other is to conduct direct analysis. Direct analysis can be divided into two categories: the method using scanning analysis tools and the method using factors. Unauthorized access is where no pre-agreed use of network or computer resources is seen as unauthorized access. It mainly has the following forms: fake identity attack, illegal users into the network system, illegal operations, legal users without authorization. Transmission of virus computer virus, through the network transmission is very destructive, and the user is difficult to prevent, seriously can paralyze the whole network.

2.3 Machine Learning Algorithm Build a Security System Model

The purpose of machine learning is to solve the dependencies between the input and output of the system based on a given training sample, enabling it to make an as accurate prediction as possible for the unknown output. Therefore, in the process of research, it is necessary to obtain the effective information contained in it from the actual data containing a large amount of useless information. Therefore, the measure of traditional

European space is difficult to use for real-world nonlinear data, which requires the use of a new treatment method for the distribution of the data. In machine learning algorithms, the generalization bound is the relationship between empirical risk and actual risk, and the specific expression formula is:

$$\eta\left(\frac{1}{\varpi}\right) = \sqrt{\frac{\varpi - \lambda^2}{\eta}} \tag{2}$$

In formula (2), η represents the number of samples, ϖ represents the dimension of the function set, and λ represents the confidence interval. The confidentiality of the network information can be guaranteed by encrypting the information. There are three main kinds of information encryption technologies: link encryption, node-to-node encryption, and end-to-end encryption. Protect the link information security between network nodes can be used link encryption, link encryption encryption data message, routing, check and other control information. However, the link encryption does not encrypt the data in the network nodes. Therefore, the node encryption technology arises. The node encryption uses the protection device installed for encryption and decryption in the middle node to realize the encryption between the nodes. In the traditional calculation method, the relationship between data and data is defined in the European space, but in practice, these data points may not be distributed in the European space, rapid development in recent years, with the development of the Internet technology, we live in the world produces a lot of data, we also filled with a lot of information, information leads to data explosion but effective knowledge is poor. Network security threats are very different. Based on the basic idea of identifying unknown factors without difference, we should not only pay attention to the traditional various types of network threats, but also pay attention to some constantly emerging and dynamically changing various types of network threats. Network security threats can come from internal and external aspects. To sum up, they can be classified into four types, as shown in Fig. 2:

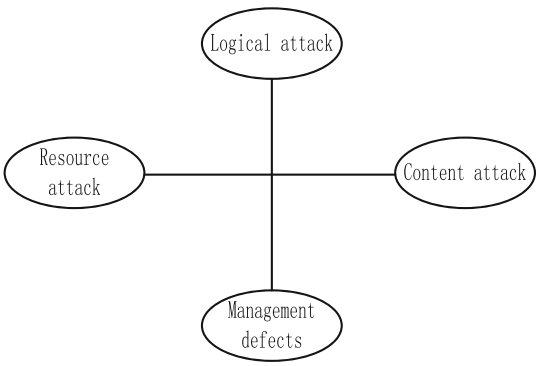

Fig. 2. Type of network security threats

As shown from Fig. 2, network security threats can be classified into logical attacks, resource attacks, content attacks, and management defects. Among them, many specific

attack threats simultaneously have a variety of attack attributes, belonging to the compound security threats. Other disasters, such as natural disasters and human error, are a special type of security threat. Although most natural disasters are force majeure, they can be prevented, avoided and reduced in many cases, so they should also be included in the category of artificial management defects.

In the process of security risk assessment of computer network information system, the components of computer network information system can be evaluated, and these components are closely related, so it is very important security in the process of risk assessment. Therefore, in the process of risk assessment, various attributes such as asset value, security events, security needs, business strategy and participation risk should be fully considered. The attack object of logical attack can be various aspects, it is to find and use the logic defects and loopholes in the existing system or application, through technical means to obtain system control rights, obtain illegal access rights, affect system performance or system functions, cause system crash, etc. Among such attacks, the public is most familiar with the various attacks against operating system vulnerabilities, such as stack overflow in Windows PnP services, ping of death attacks, red code attacks, shock wave attacks, panda incense virus attacks, which are all developed through the vulnerabilities of the system. Risk assessment can include the following contents: the relevant risk assessment agencies to develop detailed business assessment development needs strategies, and to effectively evaluate their assets. Attacks against the defects of network protocols such as TCP/IP also belong to the type of logical attacks, such as ARP deception using half-open connection to consume server resources, DNS hijacking, etc. These attacks are technically "legal", but they are illegal. Computer network information system assets use unit has relevant value, institutions to carry out specific business assets have a high degree of dependence, if the assets have very large value, so these assets will face very big risk: in the process of computer network information system execution, risk mainly includes two kinds, respectively is human risk or natural risk, assets face security events are very big threat, lead to computer network information system assets face greater risk. Common injection attacks against the databases of WEB servers are also logical attacks by exploiting vulnerabilities in the WEB service design. Other such as Trojan, spyware, password scanning attacks, also mostly to use the system or application defects to attack. Computer network threats need to be caused or generated by using system vulnerabilities or defense technology vulnerabilities, while assets have high vulnerability, and the stronger the risks faced by computer network information systems.

For the computer network information system, risk is inherent and unavoidable. People's cognition of risk is the need for security and risk assessment. The main attack object of resource attack is mainly the target system resources or network resources, such as a lot of server CPU and memory, a lot of bandwidth or connections, a lot of storage space, etc. The most typical of such attacks is the denial of service attacks, such as various Dos. Ddos (Distributed denial of service). The security requirements of assets can be adopted to ensure that the computer network information system has high security, and can ensure the inherent value of computer network assets, using computer network risk control and defense measures, in order to avoid being detected by the computer network information system. The current zombie or zombie network attacks

have been developed on this basis, which can have a variety of effects at the same time. The malicious resource occupation of viruses is also an important manifestation of resource attacks, such as spam and excessive network advertising not only waste network bandwidth and storage space, increase system memory footprint, but also waste a lot of users' working time, and may include virus attacks. Content attack is the deletion, modification, theft, deception, drowning, mining of the target, etc. Information mining for the target system is a very hidden type of attack. Computer network information system implement security protection measures, can effectively reduce the threat of assets, reduce the vulnerability of security events: implementation of computer network security measures, can reduce the threat of assets, reduce threat vulnerability, serious security risk events, so as to reduce the network information system damage as far as possible. The risk of computer network information cannot be reduced to zero. In fact, the risk cannot be reduced to zero. Therefore, it is necessary to take strict risk prevention measures to ensure that the residual risks of computer network information systems are identified and strictly control the residual risks.

2.4 Optimize the Safety Risk Assessment Mode

Information security risk assessment work is an extremely complex and extremely challenging work, heavy workload, need a lot of professional knowledge to support. Therefore, a very practical assessment tool is required for completing the risk assessment work. Traditional content attacks such as network listening, network message sniffing, etc., in recent years, some more popular content attacks, such as IP address deception, it does not change the original correct IP corresponding content, but to cheat, through technical means to get the wrong feedback results. It can not only free the technical personnel from the heavy asset statistics and risk assessment work, but also complete some work that manpower can not complete.

Risk assessment tools are an important factor to ensure the credibility of the risk assessment results. Phishing takes advantage of their psychological weaknesses by using similar domains, IP turns and other decoys to get the wrong page and the trust of visitors. According to the different focus of the risk assessment tools in the assessment activities, the risk assessment tools are divided into three categories: management risk assessment tools, technical risk assessment tools and risk assessment AIDS. Management risk assessment tool is a comprehensive assessment management tool, which focuses on security management, comprehensively considers the security risks faced by information, and finally gives corresponding control measures and solutions. Some attacks at the application layer also belong to the type of content attacks, such as malicious (rogue) software will steal user privacy, collect user habits, forcibly push non-requested content, and will consume a lot of users' system resources and working time. Such assessment tools are usually based on some kind of model or expert system. These tools are mainly divided into three categories: risk assessment tools based on information security management standards or guidelines issued by the state or government, risk assessment tools based on expert systems, and risk analysis tools based on qualitative or quantitative algorithms. The tool focuses on collecting the data and data required for evaluation and establishing the corresponding information base and knowledge base. It is a management information system that integrates various risk assessment knowledge

bases and guidelines. Spam also plays an important role in content attacks, not only forcing non-requested information, wasting bandwidth, user time and storage space, but also including attacks such as cheating and viruses.

The purpose of machine learning is to minimize the expected risk function, but the available information is the sample, so it is difficult to calculate the defined function. In order to overcome this difficulty, in practical application, empirical risk is often used instead of the expected risk function for risk calculation, in which empirical risk is defined as:

$$Y_{\mu} = \frac{1}{\mu} \sum \left\| \mu^2 - \lambda \right\| \tag{3}$$

In formula (3), μ represents the weight vector and λ represents the training sample set. With other attack types of attack source from external, management defect is due to their intentional or unintentional management defects, errors and make information system under the security threat, such as mismanaged system of internal information theft, security measures deployment is not in place or deployment error lead to other attacks, etc., these management defects objectively lead to information system attack. Commonly used risk assessment AIDS include checklists, personnel interviews, asset information questionnaire, intrusion detection tools, security audit tools, and so on.

The above three kinds of tools have different priorities. In the complex process of risk assessment, these three kinds of tools should be used comprehensively to better improve the efficiency of information security risk assessment and the correctness of the assessment results. The classification of attack types is mainly to investigate the convenience of analysis. In the actual security research, various security threats are complex, so we must identify these problems with no different unknown factors, and solve the problems with elastic closed structure ideas. Network assets include computer hardware, communication facilities, databases, document information, software, information services and personnel. Asset transfer is the evaluation of the safety value of assets. The grade appraisal of the final asset value is based on the assignment level of the confidentiality, integrity and availability of assets. After comprehensive evaluation, it can be divided into five different grades from 1 to 5. It mainly includes five stages: risk assessment preparation, risk factor identification, risk determination, risk assessment and risk control. The preparation of risk assessment, judging whether the risk is acceptable, maintaining existing control measures, and implementing risk management need to be experienced by the assessors, and the rest can be done with auxiliary tools. The higher the level, the more important the asset is. Threats to network security can be roughly divided into two types: one is the threat to information in the network. The second is the threat to network equipment. The final threat is assigned in a qualitative relative manner. The level of threat is divided into five levels, the higher the level, the more likely the threat occurs, so as to complete the assessment of network information security risk.

3 Experimental Test

3.1 Experimental Preparation

Because MIPS64 series can support up to 16 cores, efficient resource scheduling management system can dynamically allocate these cores, according to the network data

flow, arrange a certain number of cores for underlying package processing, TCP inspection, and QoS function, so as to meet the requirements of basic network data processing/firewall. The AEEEM dataset, collected by D'Ambros et al., contains information about five Eclipse projects supporting the Eclipse network projects Eclipse Kura, Ecfipse Paho and EclipseOM2M, each including several samples with one software module in each sample. The information database adopts the SQL Server2020 database under the Windows platform, which not only covers the evaluation elements of various evaluation criteria, but also can provide customers with standard evaluation application, questionnaire survey and other forms, but also provides previous evaluation experience, historical data and expert experience for the risk assessment process. The system will also arrange a certain number of cores to complete the encryption and decryption function of network data to meet the needs of VPN function. At the same time, a certain number of cores should be arranged for packet depth detection to meet the requirements of intrusion prevention and intrusion management function (IMS/IPS).The knowledge base can also enrich the information database by accepting the risk information collected by the client machine and the evaluation results of the application server. Each software module consists of 61 attributes, containing information based on the software code, development process, entropy, biweekly system resolution, historical information extracted from the cvs logs, etc. Running environment: the computer is configured with a CPU of 2.80 GHz, 215 MB of memory, Windows XP environment, V C++ 6.0 version compiled toolbox. The operating environment of ANN is: the computer is configured with a CPU of 2.80 GHz, 215 MB of memory, and Windows XP environment, MATLAB.

3.2 Experimental Results

To test the effectiveness of this design method, the experimental test was conducted. Literature [6] and literature [7] methods were selected as comparison methods for experimental comparison. The accuracy rates of the three network information security risk assessment methods were tested with different numbers of training samples. The experimental results are shown in Table 1–4:

Table 1. Training sample 20 accuracy (%)

The number of experiments	Literature [6] methods	Literature [7] methods	This article, method
1	84.646	86.144	92.613
2	85.314	85.991	91.808
3	86.002	81.205	90.554
4	84.997	86.717	92.617
5	85.131	84.310	89.665
6	84.206	85.441	92.388
7	85.449	86.212	93.445

(*continued*)

Table 1. (*continued*)

The number of experiments	Literature [6] methods	Literature [7] methods	This article, method
8	86.778	85.411	94.618
9	85.001	82.337	95.612
10	86.314	85.912	93.005
11	86.188	83.776	94.119
12	85.474	83.210	93.552
13	86.313	84.914	94.663
14	85.909	80.208	93.574
15	84.555	82.494	92.151

Table 2. Training sample 80 accuracy (%)

The number of experiments	Literature [6] methods	Literature [7] methods	This article, method
1	62.515	63.004	74.551
2	63.848	65.214	75.612
3	62.191	66.997	76.994
4	64.774	67.855	75.313
5	65.021	68.549	76.205
6	66.988	66.303	77.946
7	64.192	65.714	78.112
8	63.550	66.122	79.645
9	64.548	65.977	76.484
10	63.215	64.515	77.699
11	64.829	68.312	78.505
12	63.774	69.553	77.646
13	64.152	65.225	78.985
14	65.901	67.306	79.633
15	66.324	64.121	75.001

3.3 Experimental Analysis

From Table 1, At the training sample of 20, The designed network information security risk assessment method, The average accuracy of the other two network information security risk assessment methods is 92.959%, 85.485% and 84.285% respectively; From Table 2, At the training sample of 80, The designed network information security risk

Table 3. Training sample 150 accuracy (%)

The number of experiments	Literature [6] methods	Literature [7] methods	This article, method
1	56.948	55.649	66.588
2	57.644	56.344	67.915
3	58.499	55.124	66.922
4	57.214	56.942	65.212
5	58.331	55.812	66.748
6	57.029	56.919	65.201
7	58.677	55.701	66.339
8	57.123	56.228	65.201
9	56.911	55.322	66.819
10	55.744	57.415	63.155
11	56.998	56.021	64.498
12	55.303	55.947	62.815
13	56.472	56.319	61.402
14	55.988	57.414	60.994
15	56.461	55.168	59.166

Table 4. Training sample 300 accuracy (%)

The number of experiments	Literature [6] methods	Literature [7] methods	This article, method
1	32.152	33.144	52.131
2	36.519	34.505	49.878
3	35.597	36.917	53.009
4	34.008	35.222	49.677
5	33.455	34.919	51.088
6	34.813	35.060	52.119
7	35.914	36.977	53.477
8	36.477	34.181	49.512
9	35.219	35.199	48.667
10	36.088	34.162	47.101
11	35.164	36.121	46.922

(*continued*)

Table 4. (*continued*)

The number of experiments	Literature [6] methods	Literature [7] methods	This article, method
12	35.007	32.849	45.833
13	34.151	33.744	50.004
14	33.088	38.542	52.825
15	33.121	32.179	51.147

assessment method, The average accuracy rate of the other two network information security risk assessment methods is 77.222%, 64.388% and 66.318% respectively; From Table 3, At the training sample of 150, The designed network information security risk assessment method, The average accuracy rate of the other two network information security risk assessment methods is 64.598%, 57.023% and 56.155% respectively; From Table 4, At a training sample of 300, The designed network information security risk assessment method, The average accuracy rate of the other two network information security risk assessment methods is 50.226%, 34.718% and 34.915% respectively.

4 Conclusion

The previous computer network information security risk assessment methods have the problems of low assessment accuracy, which seriously restricts the assessment effect. In order to solve this problem and improve the effect of network information security risk assessment and the level of network information security, this paper analyzes the basic principles and analysis steps of the computer network information system security risk assessment method. This method takes non differential identification of unknown factors as the object, does not forcefully divide risk factors and non risk factors, that is, non differential identification of unknown factors. Through time, environment, object and dynamic transformation, The unknown factors are transformed from a whole into a ring-shaped closed structure. This paper introduces in detail the specific characteristics and existing problems of the introduction of machine learning algorithm into the traditional network information security risk assessment method, so as to reduce the impact of assessment factors, improve the objective accuracy of risk assessment, greatly reduce the blind areas and errors of risk assessment, and determine the determination principles and methods of unknown factors, which can solve the problems existing in the current computer network information security risk assessment, To help ensure the information security of the computer network.

References

1. Mao, Z., Hong, M., Xiao, Y., et al. Risk assessment of smart city information security based on bayesian network. Mod. Inf. **40**(5), 19–26, 40 (2020)
2. Kong, S., Zhao, Y.: Research on web-based network information security risk assessment model. China Comput. Commun. **32**(9), 200–202 (2020)
3. Liao, Y., Wang, J., Tian, K., et al.: Dynamic information security risk assessment for railway signaling safety data network based on Bayesian inference. J. China Railway Soc. **42**(11), 84–93 (2020)
4. Ren, J.-W.: Research on AHP model of computer network information security risk. Adhesion **43**(9), 157–160 (2020)
5. Liu, D.-W.: Risk assessment of network security technology based on fuzzy MCDM. Inf. Technol. **10**, 82–86 (2020)
6. Liu, J., Meng, X.: Survey on privacy-preserving machine learning. J. Comput. Res. Dev. **57**(2), 346–362 (2020)
7. Wang, Y., Liu, L.F., Huang, D.Z.: Simulation of network information trustworthiness based on machine learning algorithm. Comput. Simul. **37**(8), 239–242, 445 (2020)